Datenschutz und Robotik – Eine Einführung

Gastautor 2016-06-22T09:00:03

von BERTHOLD HAUSTEIN

Auf einer Tagung 2012 in Bielefeld fiel der aphoristische Satz: „Roboter sind auch nur Kameras auf Rädern“. Damit ist das Problem gut auf den Punkt gebracht: Roboter, vor allem solche, die sich bewegen, sind auf umfangreiche Umgebungsdaten angewiesen. Das ruft den Datenschutz auf den Plan. Einige der Fragen rund um die datenschutzrechtliche Behandlung von Robotern sollen hier dargestellt werden.

Roboter haben Sensoren, Sensoren sammeln Daten. Diese Sensordaten können auf unterschiedliche Weise gewonnen werden: per Infrarot, per Laser und nicht selten durch das Filmen der Umgebung mit Kameras. Die anfallende Datenmenge ist gewaltig und nicht wenige dieser Daten sind personenbezogen. Gesichter, Nummernschilder, Betriebs-IDs, Arbeitszeiten und vieles mehr können in die Datenwolke eines Roboters eingespeist und dort verarbeitet werden.

Robotik und datenschutzrechtliche Systematik

Allerdings finden die modernen technischen Entwicklungen und das System des Datenschutzrechtes nur bedingt zueinander. Das Datenschutzrecht arbeitet mit einem Schwarz-Weiß-Prinzip unter dem prosaischen Namen „Verbot mit Erlaubnisvorbehalt“. In § 4 Abs. 1 BDSG ist festgelegt, dass die Verarbeitung personenbezogener Daten (grundsätzlich) verboten ist, wenn sie nicht (im Einzelfall) gestattet ist oder der von den Daten Betroffene in sie eingewilligt hat. Das bedeutet, dass für jedes Datum eine Prüfung anzustellen ist: Handelt es sich um ein personenbezogenes Datum und wenn ja, gibt es für die Verarbeitung eine Rechtsgrundlage oder eine Einwilligung. Für einen Roboter mit all seinen Datensätzen, die er sekundenschnell in Echtzeit verarbeitet, ist dies eine nicht zu bewältigende Aufgabe. Dazu kommt, dass nicht bis ins letzte geklärt ist, wann das vom Roboter vorgenommene Datensammeln, Auswerten und unter Umständen Löschen innerhalb von Sekunden dem Betreiber des Geräts als Datenverarbeitung personenbezogener Daten zuzurechnen ist. Kann der Betreiber überhaupt auf die Daten zugreifen oder sind sie hermetisch im technischen System gefangen („in-the-box“)? Ist ein Zugriff durch eine verantwortliche Stelle überhaupt vorgesehen und wie kompliziert gestaltet er sich im Einzelfall? Dies sind Fragen, die in datenschutzrechtliche Verhältnismäßigkeitsprüfungen eingestellt werden müssen und in hohem Maße von der genauen Ausgestaltung eines Roboters abhängen. Ein

Umstand, der in der Praxis auch Kommunikationsbarrieren zwischen Juristen und Ingenieuren deutlich werden lässt.

So wenig Daten wie möglich, so viele Daten wie nötig

Ein weiterer, tief in der rechtlichen Systematik angelegter Konflikt entsteht dadurch, dass das Datenschutzrecht die verantwortlichen Stellen auf das Prinzip der Datensparsamkeit verpflichtet (§ 3a BDSG), während aus zivilrechtlicher, d.h. haftungsrechtlicher Perspektive umfangreiche Dokumentationen angezeigt sind. Als Beispiel mag das autonome Fahrzeug dienen, denn letztlich handelt es sich auch bei ihm um einen „Mobilitätsroboter“. Diese sind mit rund-um-Kameras ausgestattet und mit event data recorders. Es ist nur naheliegend auch die Umgebungsaufnahmen der Kameras in einer Black-Box zu speichern, um in Haftungsfällen die Kausalverläufe besser nachvollziehen zu können. Das kann für den Fahrer gelten, der sich exkulpieren will oder ein Mitverschulden beweisen. Noch viel mehr gilt es aber für den Hersteller des (autonomen) Pkw, der durch die Daten des Fahrzeuges und der Umgebung Fehler in seinem Produkt finden kann (und muss) oder beweisen will, dass Unfälle nicht auf ein Versagen der von ihm gebauten Technik zurückzuführen sind. Aus dieser Perspektive sind also so viele Daten wie möglich wünschenswert.

Wer verdient mit Daten Geld?

Nicht nur in Fallkonstellationen autonomer Fahrzeuge stellt sich zudem eine weitere Frage: Für personenbezogene Daten sieht das Datenschutzrecht ein Abwehrrecht vor, dass das Allgemeine Persönlichkeitsrecht des Betroffenen schützt. Für nicht personenbezogene Daten gibt es dagegen kaum einen rechtlichen Rahmen. Gerade diese Daten werden aber zunehmend wirtschaftlich relevant. Die Logs eines Industrieroboters können unter Umständen einen erheblichen wirtschaftlichen Wert darstellen, da sie das Rohmaterial sind, mit dem Arbeitsabläufe verbessert werden können (zum Beispiel mit Big-Data-Analysen) oder Fehler gefunden und behoben. Dieser wirtschaftliche Wert entsteht durch die Nutzung eines Roboters, egal ob autonomer Pkw, Industrieroboter, Serviceroboter oder anderes. Für die vom Recht konturierte Güterordnung stellt sich damit die Frage, wem dieser wirtschaftliche Wert zugewiesen wird. Wem „gehören“ die „Früchte“, die sich aus der Nutzung eines Geräts ergeben? Verhandelt wird diese Frage und den Schlagwörtern „Dateneigentum“ und „data ownership“.

Sektoraler Datenschutz zum Beispiel für Arbeitnehmer

Das Normdickicht des Datenschutzrechtes wird noch undurchdringlicher, wenn es um Datenverarbeitungen in Arbeitsverhältnissen geht. Das liegt zum einen daran, dass es Sondervorschriften für Arbeitsverhältnisse im Datenschutzrecht und außerhalb gibt (bspw. § 87 Abs. 1 Nr. 6 BetrVG), zum anderen daran, dass die Möglichkeiten einer datenschutzrechtlichen Einwilligung in Arbeitsverhältnissen begrenzt sind. Anders als bei anderen Vertragstypen geht man bei Arbeitsverträgen davon aus, dass das Machtverhältnis zwischen den Vertragsparteien deutlich einseitig zu Gunsten des Arbeitgebers ausgestaltet ist,

weswegen an datenschutzrechtliche Einwilligungen hier besondere Anforderungen gestellt werden. Auch und besonders in Arbeitsverhältnissen in der Industrie bekommt der Datenschutz durch die Entwicklung moderner Robotik eine verstärkte Bedeutung. Insbesondere wenn Arbeitnehmer mit den Geräten interagieren sollen (Mensch-Maschine-Interaktion), müssen und werden die Maschinen auch – schon aus Sicherheitsgründen – Daten des Arbeitnehmers erfassen. Daraus lassen sich unter Umständen auch konkrete Rückschlüsse auf dessen Leistung im Betrieb ziehen, was zu einer vom Gesetzgeber nicht gewollten Überwachungssituation führen kann.

Datenschutz zwischen Deutschland und Europa

In eine ganz neue Situation geraten Hersteller und Betreiber von Robotern zuletzt durch die weitere Europäisierung des Datenschutzes durch die erst kürzlich verabschiedete Datenschutzgrundverordnung der EU. Die abschließende Harmonisierung des Datenschutzes in Europa wurde immer wieder auch aus der Wirtschaft angeregt und gefordert, um die unterschiedlichen datenschutzrechtlichen Standards in Europa in den Griff zu kommen. Diesem Ziel dürfte mit der Verordnung entsprochen worden sein. Allerdings lässt die Verordnung doch auch einigen Interpretationsspielraum zu, der sich erst mit zunehmender Judikatur in den nächsten Jahren und Jahrzehnten verengen wird. Dort, wo sich diese datenschutzrechtliche Unschärfe auf die hohen Haftungsrisiken robotischer Anwendungen trifft, kann sie für Hersteller und Betreiber von Robotern unangenehm werden.

Datenschutz als legislative Herausforderung

Das Datenschutzrecht wirkt aber nicht nur auf die Robotik, es gibt auch Entwicklungen in die andere Richtung. Ursprünglich technische Konzepte – wie *privacy by design* und *by default* – haben mittlerweile in der Grundverordnung Eingang in die Gesetzgebung gefunden. Dies ist auch Ausdruck davon, dass der Gesetzgeber verstanden hat, dass die effektive Verwirklichung eines als Persönlichkeitsschutz verstandenen Datenschutzes nur funktionieren kann, wenn er zu einem nicht unerheblichen Maße *technischer* Datenschutz ist. Regeln, die an den technischen Gestaltungen vorbeigehen, werden auf die Dauer entweder von sich aus leer laufen oder umgangen werden.

Datenschutzrecht funktioniert – das ist vielleicht einer seiner Fehler – überall gleich: Die Weihnachtskartenadressliste des Uhrmachers und der autonome und mobile Industrieroboter unterliegen weitgehend den gleichen Regeln. Abschließend lässt sich also sagen, dass es keine prinzipiellen, systemischen Unterschiede gibt. Schaut man aber genau hin, fallen doch einige besondere Konstellationen auf, die eine Beschäftigung mit Fragen an der Schnittstelle von Robotik und Datenschutz reizvoll erscheinen lassen.
